

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY  
DOCUMENT  
ELECTRONICALLY FILED  
DOC #:  
DATE FILED: 6/24/2024

UNITED STATES OF AMERICA,

-against-

BORIS AMINOV, CHRISTY CORVALAN, IRINA  
POLVANOV, ROMAN SHAMALOV, ANTONIO  
PAYANO, DAVID FERNANDEZ, CRYSTAL  
MEDINA, JUAN HERNANDEZ, a/k/a “Pop,” and  
ALBERT YAGUDAYEV, a/k/a “Jeff,”

Defendants.

1:23-cr-110-MKV

**ORDER DENYING**  
**DEFENDANT YAGUDAYEV’S**  
**RENEWED MOTION**  
**TO SUPPRESS**

MARY KAY VYSKOCIL, United States District Judge:

This multi-defendant criminal action charges various defendants with participating in an alleged HIV prescription drug diversion scheme by which certain defendants sold diverted, black-market HIV medication to certain other defendants, who then knowingly distributed that medication to patients through the pharmacies they owned and operated, while billing Medicaid, Medicare, and private insurance companies for full value of the medication. Currently before the Court is Defendant Albert Yagudayev’s motion to suppress (the “Motion”) pursuant to Federal Rule of Criminal Procedure 12 and the Fourth Amendment, which seeks to suppress evidence obtained following the execution of an October 27, 2023 Electronically Stored Information (“ESI”) search warrant (the “Search Warrant”). [ECF No. 204]. For the reasons set forth below, the motion is DENIED.

**BACKGROUND**

On October 17, 2023, a Grand Jury returned a sealed superseding indictment (the “Superseding Indictment”) charging Defendant Yagudayev with conspiracy to violate the Anti-Kickback Statute and charging other co-defendants with wire and healthcare fraud; mail fraud;

conspiracy to defraud the United States; and money laundering in connection with the alleged black-market HIV prescription diversion scheme.

On October 18, 2023, Magistrate Judge Cott issued a warrant authorizing, among other things, the search and review of Cellphone Location and Pen Register Information of a cellphone alleged to belong to Defendant Yagudayev (the “Cellphone Location Warrant”). *See* Declaration of Anthony M. La Pinta (“La Pinta Decl.”), Exhibit A.

Shortly thereafter, on October 27, 2023, Magistrate Judge Parker issued an ESI warrant authorizing, among other things, the search and review of electronically stored information kept on a cellphone allegedly belonging to Defendant Yagudayev (the “Search Warrant”). *See* La Pinta Decl., Exhibit B. The Search Warrant—the warrant Defendant now challenges in his Motion—was issued based on an over-twenty-page affidavit submitted by Special Agent Christopher Marsh of the United States Department of Health and Human Services Office of the Inspector General (the “Affidavit”). *See* La Pinta Decl., Exhibit B. In sum, the Affidavit sought to establish probable cause to search “an Apple iPhone with a home screen background depicting a necklace of Greek ‘Evil Eyes’ that had been seized from [Defendant Yagudayev]” during his October 20, 2023 arrest. *See* Affidavit at Attachment A.

In particular, the Affidavit set forth facts supporting probable cause to believe that Defendant Yagudayev had engaged in the “Subject Offenses,” which the Affidavit defined as violations of Title 18, United States Code, Sections 1343 and 1349 (conspiracy to commit wire and health care fraud) and 371 (conspiracy to violate the Anti-Kickback Statute and to defraud the United States) (collectively, the “Subject Offenses”). *See* Affidavit at 5. These facts included, *inter alia*, a discussion of the Superseding Indictment charging Defendant Yagudayev with conspiracy to violate the Anti-Kickback Statute following his pharmacy’s purported payment of

cash kickbacks to a confidential informant on several occasions, one of which was audio and video recorded. *See* Affidavit at 5–6. Moreover, the Affidavit detailed Defendant Yagudayev’s work as a manager of FamilyRX pharmacy, which the Government believes has engaged in the same HIV medication billing scheme that is the subject of the Superseding Indictment. *See* Affidavit at 5–8. The facts further included an analysis of Defendant’s bank records; physical surveillance; interviews with employees of FamilyRX; and other documents, all detailing probable cause to believe that Defendant Yagudayev, in his role as the manager of FamilyRX, participated in the charged HIV medication diversion scheme. *See* Affidavit at 5–8.

In addition, the Affidavit set forth facts supporting probable cause to believe that Defendant Yagudayev’s cellphone (described throughout the Affidavit as the “Subject Device”) contained “evidence, fruits and instrumentalities” of the Subject Offenses. The Affidavit relied on several facts particular to this case, including that Defendant Yagudayev had used his cellphone to communicate with the confidential informant to whom he paid a cash kickback and that Defendant Yagudayev had identified the cellphone as his at the time of his arrest and provided agents with his PIN code. *See* Affidavit at 11. Moreover, Special Agent Marsh also detailed various points with respect to the use of cellphones in the commission of criminal conduct such as that charged in the Superseding Indictment. Affidavit at 12–14. The Affidavit then listed various “sub-categories” of evidence likely to be found on Defendant Yagudayev’s cellphone. *See* Affidavit at 15–16.

Defendant Yagudayev now moves to suppress all evidence obtained following the execution the Search Warrant. [ECF No. 204 (“Def. Mem.”)]. The Government filed a brief in opposition [ECF No. 213 (“Gov. Opp.”)], and Defendant Yagudayev filed a reply brief [ECF No.

219] (“Reply”). The Court has carefully reviewed all the submissions, including the Affidavit supporting the challenged Search Warrant.

### **DISCUSSION**

“[T]he Fourth Amendment provides that ‘a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity.’ ” *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Kentucky v. King*, \_\_\_ U.S. \_\_\_, 131 S.Ct. 1849, 1856 (2011)). Thus, the Warrants Clause both “requires particularity and forbids overbreadth.” *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 450 (S.D.N.Y. 2013); *see United States v. Purcell*, 967 F.3d 159, 178 (2d Cir. 2020). “Although somewhat similar in focus, these are two distinct legal issues: (1) whether the items listed as to be *seized* in the warrant were *overbroad* because they lacked probable cause and (2) whether the warrant was sufficiently *particularized* on its face to provide the necessary guidelines for the *search* by the executing officers.” *United States v. Hernandez*, No. 09 Cr. 625 (HB), 2010 WL 26544, at \*7 (S.D.N.Y. Jan. 6, 2010); *Purcell*, 967 F.3d at 178; *see also United States v. Dinero Express, Inc.*, No. 99 Cr. 975, 2000 WL 254012, at \*8–9 (S.D.N.Y. Mar.6, 2000) (separately analyzing particularity and overbreadth); *United States v. Cohan*, 628 F. Supp. 2d 355, 359 (“A warrant . . . can be unconstitutionally infirm in two conceptually distinct but related ways: either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries.”); *Zemlyansky*, 945 F. Supp. at 450.

#### **I. Overbreadth**

As a threshold matter, the Court notes that in Defendant’s Memorandum of Law in Support, he initially raised an “overbreadth” argument with respect to the contested Search Warrant. *See e.g.*, Def. Mem. at 4, 6, 7. However, as correctly noted by Government in its Opposition (*see Opp.*

at 12–13), Defendant’s initial “overbreadth” argument did not contend that the probable cause assertion in the Warrant does not match the scope of the search authorized. Instead, Defendant principally argued that the Search Warrant is “overbroad” because it authorized law enforcement to search and “rummage through” his “entire life.” Mot. at 7. However, in light of the aforementioned distinction between particularity and overbreadth, Defendant’s originally raised overbreadth argument is, in fact, more properly characterized as a particularity argument—“whether the warrant was sufficiently particularized on its face to provide the necessary guidelines for the *search* by the executing officers.” *Hernandez*, 2010 WL 26544, at \*7.

Indeed, after the Government made this precise point in its Opposition, Defendant’s subsequent Reply Memorandum entirely abandoned any mention of an overbreadth argument and exclusively addressed the Fourth Amendment’s particularity requirement. *See* Reply. In his Reply, Defendant concedes that his suppression motion is “*not* an issue of confusing the seizure of the cell phone itself”—*i.e.*, an overbreadth challenge. Reply at 4. Instead, Defendant clarifies that “what is contested here is the ESI warrant’s ‘catch all’ language that allows investigators unrestrained ‘exploratory rummaging in [defendant’s] belongings and the scope of the *search* is not properly set out with *particularity*.” Reply at 4–5 (emphasis added).

Accordingly, the Court addresses Defendant’s sole challenge to the Search Warrant—lack of particularity—below.

## **II. Particularity**

As stated above, Defendant argues that certain “catch-all” language in the Search Warrant failed to properly particularize the scope of the search for Defendant’s cellphone. Reply at 4–5. Specifically, Defendant challenges the language in the Search Warrant which states “[d]epending on the circumstances, however, law enforcement personnel may need to conduct a complete review

of *all* the ESI from the Subject Devices to locate all data responsive to the warrant.” Defendant argues that such “catch-all” language allowed investigators to conduct an “unrestrained ‘exploratory rummaging in [defendant’s] belongings” and therefore “the scope of the search [was] not properly set out with particularity.” Reply at 5 (quoting *Galpin*, 720 F.3d at 445).

To satisfy the Fourth Amendment’s particularity requirement, a warrant must (1) “identify the specific offense for which law enforcement have established probable cause,” (2) “describe the place to be searched,” and (3) “specify the items to be seized by their relation to designated crimes.” *Purcell*, 967 F.3d at 178. “It is familiar history that indiscriminate searches and seizures conducted under the authority of ‘general warrants’ were the immediate evils that motivated the framing and adoption of the Fourth Amendment.” *Payton v. New York*, 445 U.S. 573, 583 (1980). Those general warrants “specified only an offense,” leaving “to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.” *Steagald v. United States*, 451 U.S. 204, 220 (1981).

Indeed, where, as here, the property to be searched is electronic data, “the particularity requirement assumes even greater importance.” *Galpin*, 720 F.3d at 446. “A general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be ‘akin to a residence in terms of the scope and quantity of private information [they] may contain.’ ” *United States v. Ulbricht*, 858 F.3d 71, 100 (2d Cir. 2017), *abrogated on other grounds by Carpenter v. United States*, 585 U.S. 296 (2018) (quoting *Galpin*, 720 F.3d at 446). Notwithstanding these heightened privacy concerns, “[t]he Fourth Amendment does not require a perfect description of the data to be searched and seized.” *Ulbricht*, 858 F.3d at 100. In other words, given the nature of electronic evidence, “[s]earch warrants covering digital data may contain some ambiguity . . . so long as law enforcement agents have done the best that could

reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.” *Galpin*, 720 F.3d at 446.

Here, the Search Warrant “identif[ies] the specific offense[s] for which law enforcement ha[d] established probable cause,” *Purcell*, 967 F.3d at 178, which Defendant again does not appear to dispute. *See* Reply at 4–5. Next, the Search Warrant undisputedly describes “the place to be searched,” *Purcell*, 967 F.3d at 178, namely, “an Apple iPhone with a home screen background depicting a necklace of Greek ‘Evil Eyes’ that had been seized from [Defendant Yagudayev]” during his October 20, 2023 arrest. *See* Affidavit at Attachment A. Then, within that cellphone, the Search Warrant further authorizes investigators to review only the ESI that was created, sent, received, obtained, opened, modified, or saved (1) between August 1, 2019 and the Warrant’s execution date, and (2) for evidence, fruits, and instrumentalities of the Subject Offenses. *See* Affidavit. For further direction, the Search Warrant lists several categories that constitute evidence, fruits, and instrumentalities of the Subject Offenses, with those categories tying to specific facts of this case. *See* Affidavit at 21. The authorized categories include “SMS/MMS messages, data messages, and messages sent via other chat applications;” “address books or contact list information;” “digital photographs and videos;” “calendar, note, password, dictionary or other scheduling information;” “social media” entries; “internet or browser entries or history;” and “bank records” among other evidence. *See* Affidavit at 20–21.

Moreover, the Search Warrant contains the additional constraint that “[l]aw enforcement personnel [] make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant.” *See* Affidavit at 22. In particular, the Search Warrant specifies several techniques law enforcement could use in order to determine *which* ESI, among the large

volume of data on the cellphone, contains evidence or fruits of the Subject Offenses. These techniques include: surveying directories or folders and the individual files they contain; conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; “scanning” storage areas for deliberately hidden files; and performing electronic “keyword searches” through electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. *See* Affidavit at 20.

While there may indeed be broad language within the list of cellphone data to be searched, “a search warrant does not necessarily lack particularity simply because it is broad.” *Ulbricht*, 858 F.3d at 100; *see also United States v. Riley*, 906 F.2d 841, 844–45 (2d Cir. 1990) (“[A]llowing some latitude [regarding the warrant’s description of the category of items to be seized] simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked ‘drug records.’ ”). Defendant cites to *Galpin* for the proposition that using “catch-all language” such as “any” or “all” is overbroad. *See* 720 F.3d at 446–47, 449–50. But the Second Circuit has since held that using broad language in reference to phone data like “any” or “all” does not necessarily violate the particularity requirement. *See United States v. Romain*, 678 F. App’x 23, 26 (2d Cir. 2017) (“*Galpin* does not hold that the use of the phrase ‘any and all’ in a warrant is impermissible. In *Galpin*, we observed that the items listed in the warrant were wholly unrelated to the only offense that law enforcement had probable cause to believe the defendant had committed . . . ”).

Here, despite language like “all” being used in the Search Warrant, the Warrant does describe the sought-after items with sufficient particularity. At bottom, the Search Warrant authorizes law enforcement to “determine which files or other ESI contain evidence or fruits of



the Subject Offenses” by “surveying directories or folders and the individual files they contain,” “conducting a file-by-file review by ‘opening’ or reading the first few ‘pages’ of such files,” “‘scanning’ storage areas to discover and possibly recover deleted data,” and “performing electronic keyword searches through all electronic storage areas” for a *discrete* period of time (directly corresponding to the alleged commission of the Subject Offenses), and in a manner of making “reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant.” *See* Affidavit at 19–22.

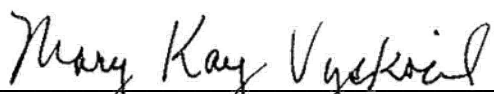
Ultimately, the Court finds that the Search Warrant is sufficiently particular to “enable the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize.” *United States v. McDarrah*, 351 F. App’x 558, 561 (2d Cir. 2009) (summary order) (quoting *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992)). While the Search Warrant concededly, “may contain some ambiguity . . . law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.” *Galpin*, 720 F.3d at 446.

### **CONCLUSION**

The Court has considered all of the arguments raised and has concluded that none warrants the suppression of evidence or a hearing. For the foregoing reasons, Defendant Albert Yagudayev’s motion to suppress evidence obtained following execution of the October 27, 2023 ESI Search Warrant is DENIED. The Clerk of Court is respectfully requested to terminate docket entry numbers 212, 230, 231, and 232.

**SO ORDERED.**

**Date: June 24, 2024**  
**New York, NY**

  
**MARY KAY VYSKOCIL**  
**United States District Judge**